A TAMPER-RESISTANT TRUSTED JAVA VIRTUAL MACHINE AND METHOD OF USING THE SAME

ABSTRACT OF THE INVENTION

A trusted Java virtual machine provides a method for supporting tamper-resistant applications, ensuring the integrity of an application and its secrets such as keys. The trusted Java virtual machine verifies the integrity of the Java application, prevents debugging of the Java application, and allows the Java application to securely store and retrieve secrets. The trusted Java virtual machine environment comprises a TrustedDictionary, a TrustedBundle, an optional encryption method for encrypting and decrypting byte codes, and an underlying trusted Java virtual machine. The encrypted TrustedDictionary protects data while the TrustedBundle protects programming code, allowing applications to store secret data and secure counters. The application designer can restrict TrustedBundle access to only those interfaces that the application designer explicitly exports. The open source code may optionally be encrypted. Secrets required by the open source programming code of the application are encrypted in TrustedDictionary.